Installations- und Benutzerhandbuch - Deutsch

FUJITSU

FUJITSU Software ServerView Suite

ServerView-Agenten V7.10 für Linux

(Linux SUSE, Red Hat und Citrix XenServer)

Ausgabe April 2015

Kritik...Anregungen...Korrekturen...

Die Redaktion ist interessiert an Ihren Kommentaren zu diesem Handbuch. Ihre Rückmeldungen helfen uns, die Dokumentation zu optimieren und auf Ihre Wünsche und Bedürfnisse abzustimmen.

Sie können uns Ihre Kommentare per E-Mail an manuals@ts.fujitsu.com senden.

Zertifizierte Dokumentation nach DIN EN ISO 9001:2008

Um eine gleichbleibend hohe Qualität und Anwenderfreundlichkeit zu gewährleisten, wurde diese Dokumentation nach den Vorgaben eines Qualitätsmanagementsystems erstellt, welches die Forderungen der DIN EN ISO 9001:2008 erfüllt.

cognitas. Gesellschaft für Technik-Dokumentation mbH

www.cognitas.de

Copyright und Handelsmarken

Copyright © 1998 - 2015 Fujitsu Technology Solutions.

Alle Rechte vorbehalten.

Liefermöglichkeiten und technische Änderungen vorbehalten.

Alle verwendeten Hard- und Softwarenamen sind Handelsnamen und/oder Warenzeichen der jeweiligen Hersteller.

Inhaltsverzeichnis

1 Einleitung **5**
1.1 Architektur 7
1.2 Zielgruppen und Zielsetzung des Handbuchs 11
1.3 Technische Voraussetzungen 12
1.3.1 Letzte Änderungen/Korrekturen 12
1.3.2 Verwalteter Server 12
1.4 Änderungen gegenüber der vorigen Ausgabe 13
1.5 ServerView Suite Link-Sammlung 13
1.6 Dokumentation zur ServerView Suite 15
1.7 Darstellungsmittel 16

2 Vorbereitungen auf den verwalteten Servern **19**
2.1 BIOS und Firmware konfigurieren 20
2.1.1 Einstellungen im BIOS-Setup 21
2.2 Server konfigurieren 24
2.3 ServerView Sicherheitskonzept 26
2.3.1 Einzelne SET-Operationen verbieten 27
2.3.2 SET-Operationen generell verbieten 27
2.3.3 SET-Operationen mit Benutzer-Authentifizierung 27
2.3.4 Betriebssystemspezifische Besonderheiten bei den ServerView-Agenten 30
2.4 SNMP-Dienste konfigurieren 30
2.5 Hardware-Uhr (CMOS-Uhr) einstellen 33
2.6 Für die Treiber Monitor-Funktion erforderliche Einstellungen 34
2.6.1 Treiber Monitor-Funktion auf SLES10 und SLES11 34
2.6.2 Treiber Monitor-Funktion unter Red Hat 35
2.7 Kernelmodule für ServerView-Agenten installieren 36
2.7.1 Kernelmodule für ServerView-Agenten installieren (SUSE Linux) 36
2.7.1.1 Das Treiberkit-Image srvmagt-modules-<version>.iso abrufen 36
2.7.1.2 Das Treiberkit-Image srvmagt-modules-<version>.iso auf dem verwalteten Server bereitstellen 37
2.7.1.3 Kernelmodule aus einem Online-Repository abrufen 38
2.7.2 Kernelmodule für ServerView-Agenten installieren (Red Hat Linux) 38

2.7.2.1 Das Treiber-Disk-Image srvmagt-modules-<version>.iso abrufen . 38
2.7.2.2 Das Treiber-Disk-Image srvmagt-modules-<version>.iso auf dem verwalteten Server bereitstellen 39
2.7.2.3 Kernelmodule aus einem Online-Repository abrufen 40

3 Installation der ServerView-Agenten 43
3.1 Voraussetzungen 44
3.2 Skript-basierte Installation 46
3.2.1 Installation über die ServerView Suite DVD 2 47
3.2.2 Installation von einem Verzeichnis 48
3.3 Installation mit dem rpm-Kommando 49
3.4 Mögliche Fehlerquellen 50
3.5 ServerView-Agenten Maintenance nach der Installation 50
3.5.1 Das Skript srvmagt 50
3.5.2 Agenten konfigurieren 53
3.5.3 Verbesserte Verfügbarkeit der ServerView-Agenten 56
3.5.4 Deinstallation der ServerView-Agenten 56
3.5.5 Agenten starten und stoppen 57
3.5.6 ServerView CIM-Provider starten und stoppen 57
3.5.7 Zusätzliche Informationen 57
3.5.8 Administrativen Benutzer festlegen 58
3.5.9 Geänderte Rechnerinformation nach der Installation 60
3.5.10 Update-Installation / Kernel-Update 60
3.5.11 Berichte ausgeben mit dem Performance Manager 61
3.5.12 Temporäre Datei im Verzeichnis /tmp 62
3.5.13 Quellname von "syslog" 62
3.6 APC-USV konfigurieren 62

1 Einleitung

Der ServerView Operations Manager (kurz: Operations Manager) ist ein kostenfreies Server-Management-Modul der Fujitsu ServerView Suite. Er steht Ihnen für die zentrale Server-Administration von Industrie Standard Servern zur Verfügung, die unter den Betriebssystemen Windows und Linux (SUSE und Red Hat) laufen oder als Host für VMs (Virtual Machine) dienen, die Hypervisor wie VMware ESXi, Citrix XenServer oder Hyper-V nutzen.

Die einheitliche Verwaltung aller Server erfolgt über eine oder auch mehrere zentrale Management-Stationen, auf die Sie von jeder Arbeitsstation im Netzwerk, auf der ein gängiger Web-Browser und das Java Runtime Environment laufen, zugreifen können.

Der Operations Manager kontrolliert die Einzelsysteme einschließlich kritischer Hardware-Komponenten, wie z. B. Prozessoren, Arbeitsspeicher, Festplatten, Lüfter und Stromversorgung. Er überwacht und steuert den Energieverbrauch, analysiert die Performanz- und Auslastungsdaten und aktualisiert die Serverkonfiguration.

Zum Sicherheitskonzept des Operations Manager gehört eine rollenbasierte Benutzerverwaltung, die auf drei grundlegenden Konzepten basiert:

- globale Benutzerverwaltung mithilfe eines LDAP-Verzeichnisdienstes (Lightweight Directory Access Protocol)
- rollenbasierte Zugangssteuerung (Role-Based Access Control, RBAC)
- Single Sign-on (SSO) auf Basis eines Centralized Authentication Service (CAS)

Mit RBAC können Sie Ihr Sicherheitskonzept an der Organisationsstruktur Ihres Unternehmens ausrichten, indem Sie jeder Rolle ein aufgabenorientiertes Berechtigungsprofil zuordnen.

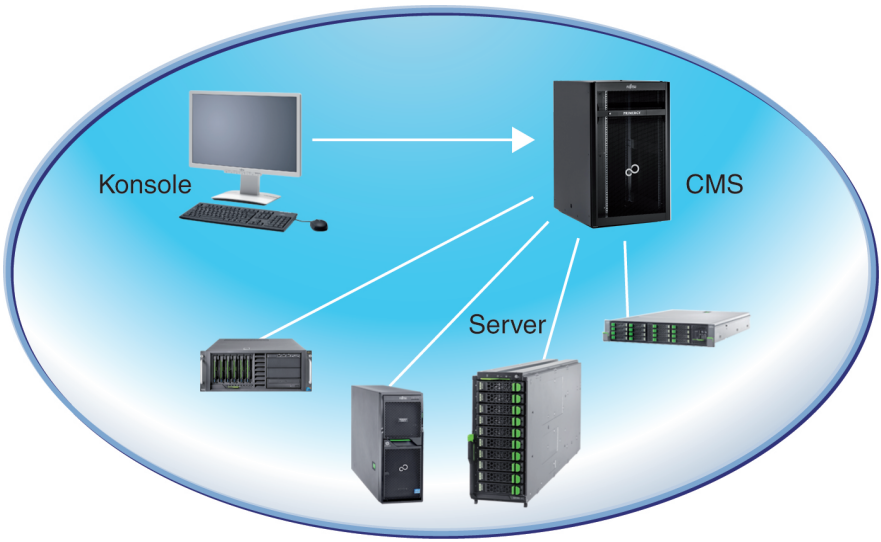
SSO bedeutet, dass Sie Ihre Authentizität nur einmal nachweisen müssen. Einmal erfolgreich authentifiziert, erhalten Sie Zugang zu allen ServerView-Komponenten, ohne sich bei einer dieser Komponenten neu anmelden zu müssen.

Das Server-Management mit dem Operations Manager bietet Betreibern eines umfangreichen Servernetzes entscheidende Vorteile:

- höhere Produktivität durch hohe Ausfallsicherheit der Server
- Senkung der Kosten durch automatisierte Überwachung der IT-Infrastruktur
- flexible Ausbaumöglichkeit der Server, da der Operations Manager problemlos an veränderte Bedingungen angepasst werden kann
- kürzere Ausfallzeiten durch vereinfachte Fehleranalyse
- Gewährleistung eines möglichst unterbrechungsfreien und energieeffizienten Serverbetriebs
- schnellere Reaktionszeiten im Falle eines Fehlers
- Senkung der Gesamtbetriebskosten (Total Cost of Ownership) durch effiziente Nutzung der Netzkomponenten und ihrer Ressourcen
- hohen Bedienkomfort durch Software-Ergonomie: übersichtliche Darstellung, intelligente Benutzerführung und unterstützendes Hilfesystem

1.1 Architektur

Die Architektur von ServerView Operations Manager basiert auf einer Management-Konsole, einer zentralen Management-Station (CMS) und den verwalteten Servern.



	Management-Konsole Eine Browser-basierte Management-Konsole ermöglicht die Verwaltung der Server und die Anzeige der ermittelten Daten. Die folgenden Browser können verwendet werden: • Microsoft Windows mit Internet Explorer oder Mozilla Firefox • SUSE/Red Hat Linux mit Standard-Web-Browser, der mit der Distribution freigegeben ist Das Java Runtime Environment muss auch installiert sein.

Zentrale Management-Station

Auf der zentralen Management-Station ist der ServerView Operations Manager installiert. Die optionalen Komponenten der ServerView Suite wie z. B. der Virtual IO-Manager werden ebenfalls auf der zentralen Management-Station installiert und in den Operations Manager integriert.

Die zentrale Management-Station und damit der ServerView Operations Manager und die zugehörigen Komponenten können auch auf einer virtuellen Maschine (VM) unter Windows oder Linux ausgeführt werden.

Das globale Benutzermanagement der ServerView Suite und des iRMC speichert die Benutzer zentral für alle zentralen Management-Stationen (CMS)/iRMC im Verzeichnis eines LDAP-Verzeichnisdienstes. Dadurch können Sie die Benutzer auf einem zentralen Server verwalten. Die Benutzer können daher von alle CMS und iRMC verwendet werden, die im Netzwerk mit diesem Server verbunden sind.

Die ServerView Suite unterstützt derzeit die folgenden Verzeichnisdienste:

- ApacheDS (unter JBoss 7).
- Microsoft Active Directory

Während der Installation von ServerView Operations Manager haben Sie die Möglichkeit, den internen Verzeichnisdienst (ApacheDS) von ServerView zu wählen. Weitere Informationen zur Nutzung der Verzeichnisdienste mit ServerView finden Sie im Handbuch "User Management in ServerView" (siehe).

Die Daten, die von ServerView erzeugt und genutzt werden, werden in einer SQL-Datenbank auf einem SQL-Server abgelegt. Die folgenden SQL-Server sind Teil der ServerView Operations Manager-Installation:

- SQL Server 2008 R2/2005 Express unter Windows Server
- PostgreSQL unter Linux

Es können aber andere Microsoft SQL Server Datenbanken unter Windows verwendet werden.

	Das Java Runtime Environment ist auf der zentralen Management-Station erforderlich. Wie Sie den ServerView Operations Manager installieren, wird in den folgenden Handbüchern beschrieben: • Installation ServerView Operations Manager Software unter Windows • Installation ServerView Operations Manager Software unter Linux
	Verwaltete Server Auf den verwalteten Servern müssen ServerView-Agenten, CIM Provider oder ServerView Agentless Service installiert sein, die die Informationen der zentralen Management-Station bereitstellen. Der ServerView RAID Manager und der ServerView Update Agent müssen auch auf den verwalteten Servern installiert werden. Die Installation der ServerView-Agenten auf virtuellen Maschinen (VMs) ist nicht freigegeben. • Die ServerView-Agenten sind verfügbar für Windows, Linux und Citrix XenServer. • ServerView CIM-Provider sind für Windows, Linux und VMware ESXi verfügbar. Der ServerView Operations Manager unterstützt aktuell nur ServerView CIM-Provider für VMware ESXi. Wie Sie diese installieren, ist in den folgenden Handbüchern beschrieben: • ServerView-Agenten für Windows • ServerView-Agenten für Linux • Installation ServerView ESXi CIM Provider • ServerView CIM-Provider für Windows, Linux und VMware ESXi

1.2 Zielgruppen und Zielsetzung des Handbuchs

Das vorliegende Handbuch wendet sich an Systemverwalter, Netzverwalter und Service-Fachleute, die über fundierte Hard- und Software-Kenntnisse verfügen. Das Handbuch beschreibt die Installation der ServerView-Agenten für Linux SUSE, Red Hat und Citrix XenServer.

1.3 Technische Voraussetzungen

1.3.1 Letzte Änderungen/Korrekturen

Eventuelle letzte Änderungen/Korrekturen der technischen Voraussetzungen finden Sie in der Readme-Datei auf der ServerView Suite DVD 2. Sie haben folgende Möglichkeiten:

- Wechseln Sie auf der DVD in das Verzeichnis **SVSSoftware** – **Software** – **ServerView** – **Linux** – **Agents**.
- Starten Sie die DVD und wählen Sie **ServerView Software Products**; Info unter **ServerView** – **Agents and Providers**.

1.3.2 Verwalteter Server

ServerView-Agenten sind verfügbar für:

- SUSE (SLES 11): SP2 und SP3
- SUSE (SLES 12)
- Red Hat Enterprise Linux 5.9/5.10/5.11
- Red Hat Enterprise Linux 6.5/6.6
- Red Hat Enterprise Linux 7.0/7.1
- Oracle Linux OL 6.5/6.6
- Citrix XenServer V6.1/6.2/6.5

1.4 Änderungen gegenüber der vorigen Ausgabe

Diese Ausgabe des Handbuchs gilt für ServerView Agents V7.10 oder höher und ersetzt das Online-Handbuch "ServerView Agents V7.00 for Linux", Ausgabe Oktober 2014.

Das Handbuch enthält die folgenden Änderungen und Erweiterungen:

- Ab Version 7.10 unterstützt ServerView Operations Manager den Verzeichnisdienst ApacheDS anstelle von OpenDJ. Deshalb wurde der Architektur-Abschnitt aktualisiert, siehe "Architektur" auf Seite 7.
- Der Abschnitt "ServerView Suite Link-Sammlung" wurde aktualisiert, siehe "ServerView Suite Link-Sammlung" auf Seite 13.
- Ab ServerView Agents V7.01 ist die ServerView System Monitor Web-Oberfläche eine neue Funktion, die zusammen mit den Agenten installiert wird (siehe "Installation über die ServerView Suite DVD 2" auf Seite 47, "Installation mit dem rpm-Kommando" auf Seite 49 und "Das Skript srvmagt" auf Seite 50).
- Ab Version 7.01 sind ServerView-Agenten in der Lage, einen Server über SNMPv3 zu überwachen. Deshalb wurde der Abschnitt "Vorbereitungen auf den verwalteten Servern" auf Seite 19 aktualisiert. Siehe auch die neue Dokumentation "Usage of SNMPv3 with ServerView Agents 7.01".

1.5 ServerView Suite Link-Sammlung

Fujitsu Technology Solutions stellt Ihnen über die ServerView Suite Link-Sammlung zahlreiche Downloads und weiterführende Informationen zur ServerView Suite und zu PRIMERGY Servern zur Verfügung.

Zur ServerView Suite werden Ihnen Links zu folgenden Themen angeboten:

- Forum
- Service Desk
- Handbücher
- Produktinformationen
- Sicherheitsinformationen

- Software Downloads
- Schulungen

Die Downloads umfassen u. a.:

  - Aktuelle Software-Stände zur ServerView Suite sowie ergänzende Readme-Dateien.
  - Informationsdateien und Aktualisierungsdateien (Update Sets) für systemnahe Software-Komponenten (BIOS, Firmware, Treiber, ServerView-Agenten und ServerView-Update-Agenten) zur Aktualisierung der PRIMERGY Server anhand des ServerView Update Managers oder für den lokalen Update einzelner Server anhand des ServerView Update Managers Express.
  - die aktuellen Versionen aller Dokumentationen zur ServerView Suite

  Die Downloads können kostenlos vom Fujitsu Technology Solutions Web-Server heruntergeladen werden.

Zu PRIMERGY Servern werden Ihnen Links zu folgenden Themen angeboten:

- Service Desk
- Handbücher
- Produktinformationen
- Ersatzteilkatalog

Zugriff auf die ServerView Suite Link-Sammlung

Die Link-Sammlung der ServerView Suite erreichen Sie über verschiedene Wege:

1. Über den ServerView Operations Manager.
   - Wählen Sie auf der Startseite bzw. in der Menüzeile **Help** – **Links** aus.

Anschließend wird die Startseite der ServerView Suite Link-Sammlung angezeigt.

2. Über die Startseite der Online-Dokumentation zur ServerView Suite auf dem Manual-Server von Fujitsu Technology Solutions.

Sie gelangen auf die Startseite der Online-Dokumentation mit folgendem Link:

http://manuals.ts.fujitsu.com

- Wählen Sie links in der Auswahlliste **x86 Servers**.

- Klicken Sie rechts unter **Selected documents** auf **PRIMERGY ServerView Links**.

Anschließend wird die Startseite der ServerView Suite Link-Sammlung angezeigt.

3. Über die ServerView Suite DVD 2.
   - Wählen Sie im Startfenster der ServerView Suite DVD 2 die Option **ServerView Software Produktauswahl**.
   - Wählen Sie in der Menüleiste **Links**.

Anschließend wird die Startseite der ServerView Suite Link-Sammlung angezeigt.

1.6 Dokumentation zur ServerView Suite

Die Dokumentation ist über das Internet als Download kostenlos erhältlich. Die Online-Dokumentation zur ServerView Suite finden Sie unter http://manuals.ts.fujitsu.com unter dem Link **x86 Servers**.

Einen Überblick über die Dokumentation zur **ServerView Suite** und die Dateistruktur erhalten Sie auf der ServerView Suite-Sitemap (**ServerView Suite – Site Overview**).

1.7 Darstellungsmittel

Es werden folgende Darstellungsmittel verwendet:

Darstellungsmittel	Bedeutung
	Weist auf Gefahren hin, die zu Gesundheitsgefährdung, Datenverlust und Geräteschäden führen können.
	Verweist auf weiterführende Informationen und Tipps.
Fette Schrift	Kennzeichnet Bildschirmzitate der Namen der Oberflächenelemente.
`dicktengleich`	Kennzeichnet Ausgaben des Systems und Systemelemente wie Dateinamen oder Pfade.
`dicktengleich halbfett`	Kennzeichnet Anweisungen, die Sie über die Tastatur eingeben.
blauer, unterstrichener Text	Kennzeichnet einen Link zu einem verwandten Thema.
lila, unterstrichener Text	Kennzeichnet einen besuchten Link.
<abc>	Kennzeichnet Variablen, die Sie durch reale Werte ersetzen müssen.
[abc]	Kennzeichnet Optionen, die Sie angeben können (Syntax).
[Taste]	Kennzeichnet eine Taste entsprechend ihrer Abbildung auf der Tastatur. Wenn Sie explizit Großbuchstaben eingeben sollen, dann wird die Shift-Taste angegeben, z. B. [SHIFT] + [A] für A. Wenn Sie zwei Tasten gleichzeitig drücken sollen, kennzeichnet dies ein Pluszeichen zwischen den Tastensymbolen.

Bildschirmabzüge
Die Bildschirmabzüge sind teilweise systemabhängig und müssen deshalb nicht in allen Details mit der Ausgabe auf Ihrem System übereinstimmen. Auch bei den Menüs und ihren Befehlen kann es systembedingte Unterschiede geben.

2 Vorbereitungen auf den verwalteten Servern

Bevor Sie den Operations Manager in Betrieb nehmen können, müssen auf dem verwalteten Server folgende Vorbereitungen getroffen werden:

- Nur für PRIMERGY: Im BIOS jedes verwalteten Servers müssen bestimmte Einstellungen vorgenommen werden, siehe "BIOS und Firmware konfigurieren" auf Seite 20.

  Auf jedem Server müssen Sie Konfigurationseinstellungen vornehmen, siehe "Server konfigurieren" auf Seite 24.
- ServerView bietet ein differenziertes Sicherheitskonzept. Bevor Sie die Agenten installieren, sollten Sie sich über das Sicherheitskonzept informieren und das Ihrem Sicherheitsbedürfnis entsprechende Konzept auswählen. Gegebenenfalls müssen Sie vor der Installation der Agenten entsprechende Vorbereitungen treffen. Dies wird beschrieben unter "ServerView Sicherheitskonzept" auf Seite 26.
- Sie müssen die SNMP-Dienste des jeweiligen Betriebssystems auf jedem verwalteten Server und der Management-Station installieren und konfigurieren. Andernfalls kann die Management-Station die Server nicht überwachen. Die SNMP-Dienste müssen je nach Betriebssystem vor bzw. nach der Agenteninstallation aktiviert werden. Dies wird beschrieben unter "SNMP-Dienste konfigurieren" auf Seite 30 .
- Ab Version 7.01 sind ServerView-Agenten in der Lage, einen Server über SNMPv3 zu überwachen.

  Zur Nutzung von SNMPv3 in der ServerView-Agenten-Kommunikation empfiehlt sich der Net-SNMP Master-Agent. Der Net-SNMP Master-Agent ist im Lieferumfang der meisten Linux-Distributionen enthalten (siehe Beschreibung unter "Usage of SNMPv3 with ServerView Agents 7.01").
- Die CMOS-Uhr muss auf die lokale Zeit eingestellt sein, nicht auf Greenwich-Zeit. Andernfalls startet der automatische Power ON/Power OFF nicht zu der konfigurierten Zeit. Dies wird in "Hardware-Uhr (CMOS-Uhr) einstellen" auf Seite 33 beschrieben.

- Die für die Treiber Monitor-Funktion erforderlichen Einstellungen müssen konfiguriert werden. Siehe "Für die Treiber Monitor-Funktion erforderliche Einstellungen " auf Seite 34.
- ServerView-Agenten müssen auf jedem zu verwaltenden Server installiert sein, siehe "Installation der ServerView-Agenten" auf Seite 43.

  Die Installation der ServerView-Agenten auf virtuellen Maschinen (VMs) ist nicht freigegeben.
- Voraussetzung für den ServerView Update Manager ist, dass auf den verwalteten Servern der ServerView-Update-Agent installiert ist. Die Installation wird beschrieben im Benutzerhandbuch "ServerView Update Management".
- Wenn der ServerView Operations Manager so konfiguriert wurde, dass der Zugriff auf die zentrale Management-Station nicht über den Namen sondern über die IP-Adresse erfolgt, muss gewährleistet sein, dass vom verwalteten Server über diese Adresse auf die zentrale Management-Station zugegriffen werden kann. Das sollte möglichst durch eine entsprechenden Eintrag in das DNS geschehen. Wenn kein DNS verfügbar ist, müssen Sie den entsprechenden Eintrag in der Datei **hosts** auf dem verwalteten Server erstellen. In Linux finden Sie diese Datei im Verzeichnis **/etc**.

Zusätzliche Installation auf den verwalteten Server

- ServerView RAID Manager

  Der ServerView RAID Manager bietet eine einheitliche Administration und Verwaltung von Festplatten für PRIMERGY Server. Ohne Installation des ServerView RAID Managers sind keine Informationen über RAID-Laufwerke und deren Zustand verfügbar.

  Die Installation ist im Benutzerhandbuch "RAID Management" beschrieben.

2.1 BIOS und Firmware konfigurieren

Die folgende Beschreibung ist nur gültig für PRIMERGY.

Abhängig von der Systembaugruppe arbeiten die verschiedenen PRIMERGY-Typen mit unterschiedlichen BIOS-Versionen. Deshalb wird auf die detaillierte

Beschreibung aller möglichen Einstellungen sowie der Bedienung des BIOS an dieser Stelle verzichtet.

Eine ausführliche Beschreibung der jeweiligen BIOS-Version finden Sie im Referenzhandbuch "BIOS Setup Utility" oder im technischen Referenzhandbuch der Systembaugruppe.

Bei der Inbetriebnahme eines Servers müssen Sie den Menüpunkt **O/S Boot Timeout** im BIOS-Setup des Systems auf **Disabled** stellen. Sonst wird das System während der Installation neu gestartet.

Erst beim Neustart des Systems, wenn alle Installationen abgeschlossen sind (einschließlich der ServerView-Agenten), können Sie den Menüpunkt **O/S Boot Timeout** auf **Enabled** stellen.

Beachten Sie außerdem, dass bei der Installation von Linux der Wert für den **Boot Timeout** so gesetzt ist, dass auch ein File System Check durchgeführt werden kann. Andernfalls wird das System während des File System Checks neu gestartet.

2.1.1 Einstellungen im BIOS-Setup

Die Server-Management-Firmware überwacht den Server, bis das Betriebssystem gestartet ist. Danach übernehmen die Agenten und der Operations Manager die Überwachungsfunktion.

Sie müssen die BIOS-Einstellungen auf jedem Server vornehmen.

Rufen Sie das BIOS-Setup auf, indem Sie den Rechner neu starten und in der Boot-Phase an entsprechender Stelle die Taste **F2DEL** oder drücken.

Wählen Sie im BIOS-Setup das Menü **Server** aus. Hier nehmen Sie die Einstellungen zum Server-Management vor.

Wird im BIOS-Setup das Menü **Server** nicht angeboten, so brauchen Sie die Server-Management-Funktionen nicht zu aktivieren. Allerdings können dann auch einzelne Server-Management-Funktionen nicht explizit gesteuert werden.

Wird im Menü **Server** der Menüpunkt **Server Management** angeboten, so wählen Sie für diesen Menüpunkt die Einstellung **Enabled** aus. Dadurch wird die

Server-Management-Funktionalität aktiviert. Alle weiteren Einstellungen werden nur dann wirksam, wenn Sie hier die Einstellung **Enabled** auswählen.

Steht der Menüpunkt **Server Management** nicht zur Verfügung, können die einzelnen Funktionen unabhängig von einer generellen Freigabe gesteuert werden.

Im Menü **Server** stehen die im Folgenden aufgeführten Felder zur Verfügung.

Beachten Sie, dass, abhängig von der Hardware, nicht alle Felder zur Verfügung stehen müssen.

O/S Boot Timeout

Hier legen Sie fest, ob ein Systemneustart erfolgen soll, wenn das Betriebssystem nach dem Systemstart nicht in einer vorgegebenen Zeitspanne Verbindung mit der Server-Management-Firmware aufnimmt.

Das Zeitintervall kann auch über den Operations Manager festgelegt werden (siehe auch im Benutzerhandbuch "ServerView Operations Manager" den Abschnitt "ASR&R").

Inbetriebnahme des Servers

Bei der Inbetriebnahme des Servers müssen Sie den Menüpunkt **O/S Boot Timeout** auf **Disabled** stellen. Sonst wird das System während der Installation neu gestartet.

Aktion nach Zeitablauf

Legt fest, welche Aktion nach Ablauf des Boot-Watchdogs ausgeführt wird.

Timeout Value

Legt die Zeit fest, nach der ein Neustart des Systems erfolgt, falls dies über **O/S Boot Timeout** eingeschaltet ist.

ASR&R Boot Delay

Legt die Zeitspanne fest, die der Server nach einer Fehlerabschaltung (z.B. wegen Übertemperatur) wartet, ehe er einen Neustart durchführt.

Boot Retry Counter

Legt fest, wie oft der Server versucht das Betriebssystem neu zu starten, bevor er abgeschaltet bleibt bzw. bevor ServerView Remote Management gestartet wird.

Diagnostic System

Legt fest, ob ServerView Remote Management gestartet wird, wenn die unter **Boot Retry Counter** eingestellte Anzahl an Systemneustarts erreicht ist.

Hardware Watchdog

Legt fest, ob der Server einen Neustart durchführt, wenn das Server-Management-BIOS einen Hardware-Zähler nicht in bestimmten Zeitintervallen zurücksetzen kann.

Next Boot uses

Legt fest, ob beim nächsten Boot-Vorgang ServerView Remote Management gestartet wird.

Temperature Monitoring

Legt fest, ob das System abgeschaltet wird, wenn die Temperatur den kritischen Wert überschreitet.

Memory Scrubbing

Legt fest, ob der Speicher überprüft und Ein-Bit-Fehler beseitigt werden.

BIOS Runtime Logging

Legt fest, ob Prozessor-, Speicher- oder PCI-Fehler in der Error-Log-Datei gespeichert werden.

CPU Status

Legt fest, ob der Prozessor verwendet werden kann.

Memory Status

Hier können bestimmte Speichermodule als fehlerhaft gekennzeichnet werden. Diese werden dann beim nächsten Systemstart nicht mehr verwendet.

Console Redirection

Legt die Einstellungen zum Betrieb eines Terminals am System fest.

RomPilot

Legt die Einstellungen zu RomPilot fest. RomPilot ist ein Bestandteil von ServerView Remote Management und des Operations Managers. Mit RomPilot ist der Remote-Zugriff von einer Remote-Konsole über LAN auf die Systemstartphase (POST) und MS-DOS möglich.

Storage Extension

Legt die Einstellungen für die Gruppenkonfiguration und den Kommunikationsbus (CAN-Bus) fest. (Hinweis: **Storage Extension** gibt es nicht auf allen Servern!)

2.2 Server konfigurieren

Zur Konfiguration von Servern stehen Ihnen verschiedene Funktionen zur Verfügung. Während einige dieser Funktionen für alle PRIMERGY Server unterstützt werden, werden andere Funktionen je nach Hard- und Software-Ausstattung der PRIMERGY Server nur für bestimmte Server angeboten.

Die Konfiguration der Server können Sie vornehmen:

- Lokal am verwalteten Server über den Server Configuration Manager.

  Mit dem Server Configuration Manager können Sie Einstellungen zum allgemeinen Systemverhalten des Zielsystems vornehmen und - sofern vorhanden - die Remote Management-Komponente (iRMC oder iRMC S2/S3) des Zielsystems konfigurieren.

  Wenn der ServerView Installation Manager über die ServerView Suite DVD 1 gestartet wird, können Sie den Server Configuration Manager über die Schaltfläche **Server Configuration Manager** starten.

  Abhängig vom PRIMERGY Server-Typ des Zielsystems werden nicht alle Schritte durchlaufen. Die Reihenfolge der einzelnen Schritte sowie die Konfigurationsmöglichkeiten in den einzelnen Schritten können ebenfalls von System zu System variieren.

Nähere Informationen zu den individuellen Schritten im Konfigurationsdialog des Server Configuration Managers finden Sie in der Online-Hilfe zum Server Configuration Manager.

Um die Online-Hilfe zu einem Schritt im Dialog aufzurufen, gehen Sie vor wie folgt:

1. Klicken Sie in den Anzeigebereich, in dem der Dialog angezeigt wird.
2. Drücken Sie die Taste F1.

- Über den ServerView Configuration Manager, der in die grafische Oberfläche des Operations Managers integriert ist. Damit können Sie den Server via Web-Interface auch vom Remote-Arbeitsplatz aus konfigurieren können.

  ServerView Configuration Manager kann über die Startseite von Operations Manager oder durch die Auswahl von **Administration** – **Server Configuration** in der Menüleiste gestartet werden.

  Weitere Informationen finden Sie im Benutzerhandbuch "ServerView Operations Manager".

  Die Konfiguration können Sie nur für Server vornehmen, auf denen die ServerView-Agenten installiert sind.

Einige der konfigurierten Einstellungen werden je nach System ins BIOS übernommen.

Sie können u.a. folgende Einstellungen vornehmen:

- Lesen der wichtigsten Daten des Servers, der Systembaugruppe und des integrierten Management Controllers
- Lesen und Setzen der Boot- und Software-Watchdog-Einstellungen
- Lesen und Bearbeiten des Fehlerzählers für die Speichermodule

Nur für PRIMERGY

- Lesen und Löschen des Error- und Event-Logs des Servers
- Überwachung und Kalibrierung der Systemlüfter
- Lesen und Setzen der Gehäusekennzeichnung (bei Auslieferung voreingestellt)
- Lesen und Zurücksetzen der Zähler über die Systemlaufzeiten

- Konfigurieren der Einstellungen für HTTP und Telnet und der Einstellung des Remote Management Controllers für HTTP
- Konfigurieren der IP- und DNS-Einstellungen der RSB Web-Oberfläche
- Konfigurieren der SNMP-Communities und der Trap-Ziele für die SNMP-Schnittstelle des Remote Management Controllers
- Verwalten der Benutzerkennungen des Remote Management Controllers
- Konfigurieren der seriellen Schnittstelle des RSBs bzw. des Remote Management Controllers
- Konfigurieren der Operations Manager USV-Management-Integration
- Konfigurieren der Anzeigen auf dem ServerView Local Service Display

2.3 ServerView Sicherheitskonzept

Die ServerView-Agenten bieten in Verbindung mit dem ServerView-Manager ein erweitertes Sicherheitskonzept, um unerlaubte SNMP-SET-Operationen auf einem Server zu verhindern.

Sie können SNMP-SET-Operationen auf dem Server einschränken. Hierbei besteht die Möglichkeit:

- einzelne SET-Operationen zu verbieten,
- SET-Operationen generell zu verbieten,
- SET-Operationen durch eine Benutzer-Authentifizierung zu schützen.

  Ist die Benutzer-Authentifizierung aktiviert, so wird vor jeder Ausführung einer SET-Operation eine Benutzer-Authentifizierung durchgeführt. Verläuft diese erfolgreich, so wird zusätzlich die Zugehörigkeit zu einer vom Administrator vergebenen Benutzergruppe überprüft.

  Die Benutzer-Authentifizierung funktioniert nur mit dem ServerView-Manager. Es ist für andere SNMP-Tools wirkungslos.

Weiterhin können Sie die Sicherheit vor unerlaubtem Zugriff erhöhen, indem Sie die Standardkonfiguration des SNMP-Dienstes ändern. Weitere Informationen finden Sie unter "SNMP-Dienste konfigurieren" auf Seite 30.

2.3.1 Einzelne SET-Operationen verbieten

Einige SET-Operationen bewirken einen Shutdown oder Neustart des Systems. Sie können diese speziellen SET-Operationen zulassen oder verbieten, siehe "Agenten konfigurieren" auf Seite 53 – AgentShut.

2.3.2 SET-Operationen generell verbieten

Sie können SET-Operationen generell für die ServerView-Agenten verbieten. Geben Sie diese Spezifikationen bei der Agenten-Installation ein, siehe "Agenten konfigurieren" auf Seite 53 – AgentPermission.

Diese Option gilt nur für ServerView-Agenten. SET-Operationen für andere SNMP-Agenten werden davon nicht beeinflusst.

2.3.3 SET-Operationen mit Benutzer-Authentifizierung

Sie haben die Möglichkeit, SET-Operationen abzusichern, indem Sie die Ausführung einer SET-Operation durch eine Benutzer-Authentifizierung absichern. Hierbei können Sie einstellen, ob die Benutzerabfrage nur zu Beginn einer Sitzung für einen Server angegeben werden muss oder bei jeder SET-Operation erneut abgefragt wird.

Für die Benutzer-Authentifizierung müssen Sie Maßnahmen auf dem verwalteten Server sowie an der Management-Station vornehmen.

Instanz	Maßnahme
Verwalteter Server	• Benutzer und Benutzergruppe festlegen • Benutzer der gewünschten Benutzergruppe zuordnen • bei der Agenteninstallation die gewünschte Benutzergruppe angeben
Management-Station	im Operations Manager auf der Registerkarte **Login** den Benutzer angeben

Benutzer und Benutzergruppe definieren und Benutzer zuordnen
Den Benutzer sowie die Benutzergruppe müssen Sie mit Betriebssystemmitteln auf dem jeweiligen Server festlegen. Sie können für den Benutzernamen sowie für die Benutzergruppe einen beliebigen Namen (z. B. auch **Administrator**) auswählen.

Vorbereitend müssen Sie sich überlegen, ob Sie für mehrere Server die gleiche Benutzerkennung und -gruppe einrichten wollen oder nicht.

Benutzergruppe bei der Agenteninstallation angeben
Bei der Agenteninstallation auf dem Server müssen Sie die Benutzergruppe angeben, zu der der Benutzer gehören muss, für den SET-Operationen zugelassen sind. Die Installation und Konfiguration der ServerView-Agenten sind je nach Betriebssystem und Version unterschiedlich. Weitere Informationen zur Installation und Konfiguration in diesen Fällen finden Sie bei den Agenten-Beschreibungen beginnend ab "Agenten konfigurieren" auf Seite 53.

Benutzer an der Management-Station angeben
An der Management-Station müssen Sie im Operations Manager den Benutzer für einen Server angeben, der SET-Operationen auf dem jeweiligen Server durchführen darf. Sie legen den Benutzer über die Registerkarte **Login** im Eigenschaftsfenster **Server Properties** fest. In diesem Beispiel wäre das der Benutzer **SVUSER**.

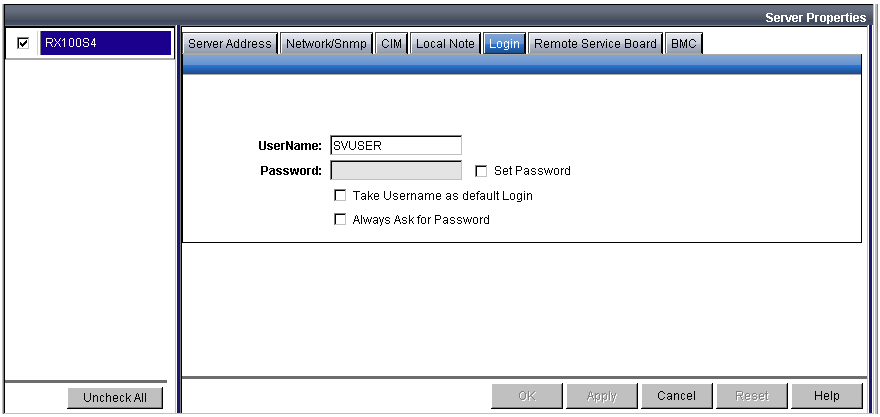


Bild 1: Benutzerkennung für die Benutzer-Authentifizierung angeben

Aus Sicherheitsgründen ist es sinnvoll, falls ein Passwort für den Benutzer vergeben wurde, das Passwort hier ebenfalls anzugeben (**Set Password**). Weiterhin legen Sie mit **Always Ask for Password** fest, ob der Benutzername und das Passwort bei jeder Änderung der Einstellungen oder nur bei der ersten Änderung nach dem Programmstart des Operations Managers abgefragt werden sollen. Sie können eine erhöhte Sicherheit erreichen, indem Sie die Funktion **Always Ask for Password** einschalten, weil in dem Fall das Passwort nicht abgespeichert wird.

Auf der rechten Spalte im Fenster **Server Properties** können Sie diejenigen Server auswählen, für die die Einstellungen gelten sollen. Sie können auch mehrere gleichzeitig auswählen. Das heißt, Sie können die Einstellungen sowohl für jeden einzelnen Server individuell als auch für mehrere Server identisch vornehmen.

Das folgende Beispiel zeigt Ihnen den Ablauf, falls eine Benutzer-Authentifizierung eingestellt wurde.

Beispiel

Der Benutzer **svuser** wurde am Server angelegt und auf der Management-Station im Operations Manager auf der Registerkarte **Login** angegeben. Bei einer SET-Operation wird dann der Benutzer abgefragt.

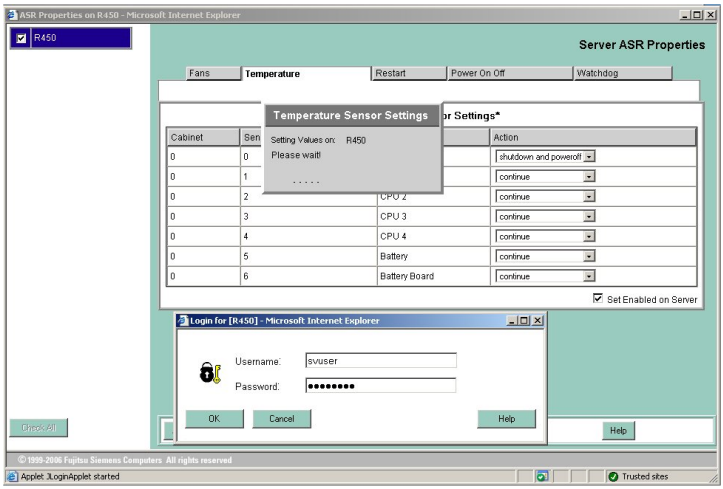


Bild 2: Benutzer-Authentifizierung

2.3.4 Betriebssystemspezifische Besonderheiten bei den ServerView-Agenten

Die folgenden Abschnitte beschreiben die betriebssystemspezifische und versionsabhängige Vorgehensweise bei der Umsetzung des Sicherheitskonzepts von ServerView.

SNMP-Sicherheitskonzept

Wenn Sie den Server über die Management-Station überwachen wollen, müssen Sie nach der Installation des Betriebssystems einen Benutzer einrichten, der zur Gruppe **bin** gehört.

Diesen Benutzer mit dem zugehörigen Benutzernamen und Passwort müssen Sie an der Management-Station eingeben, damit eine SET-Operation auf dem verwalteten Server durchgeführt werden kann.

Weitere Informationen zur Installation der Agenten finden Sie unter "Installation der ServerView-Agenten" auf Seite 43.

2.4 SNMP-Dienste konfigurieren

Sie müssen die SNMP-Dienste des jeweiligen Betriebssystems auf jedem verwalteten Server und der Management-Station installieren und konfigurieren.

Die ServerView Linux-Agenten benötigen Konfigurationsparameter in der Konfigurationsdatei des SNMP-Dienstes des Systems. Sie finden diese Datei unter dem Namen **/etc/snmp/snmpd.conf**. Sie müssen diese Konfigurationsdatei, z. B. mit Hilfe des vi, bearbeiten. Informationen zur Syntax finden Sie in den manpages zu **snmpd.conf** (Aufruf: **man snmpd.conf**).

- Geben Sie unter **sysContact** den zuständigen Betreuer und unter **sysLocation** den Standort des Servers an.

  Setzen Sie **authtrapenable** auf 1 (**enable**). So wird ein Trap gesendet, falls bei einer SET-Operation die Community der Management-Station nicht bekannt ist oder die notwendigen Rechte für die SET-Operation nicht vorhanden sind. Mit 2 (**disable**) deaktivieren Sie diese Funktion (Standardwert).

Weitere Informationen hierzu entnehmen Sie den manpages zu **snmpd.conf**.

- Das folgende Beispiel zeigt eine Konfiguration, die Sie Ihrem Netzwerk und Ihrer Serverumgebung anpassen müssen:

```
com2sec svSec localhost public
com2sec svSec <subnet>/<netmask> public
group svGroup v1 svSec
view svView included .1
access svGroup "" any noauth exact svView none none
```

  <subnet>/<netmask> müssen Sie Ihrer Umgebung entsprechend anpassen. Standardmäßig sind nur lesende SNMP-Zugriffe zugelassen.

  Wenn Sie mehr als zwei **com2sec**-Definitionen benutzen, dann ist die Reihenfolge von Bedeutung. Die erste **com2sec**-Definition, die mit der IP-Adresse und der Community eines eingehenden SNMP-Requests übereinstimmt, wird genommen. Deshalb müssen Sie die **com2sec**-Definitionen für spezifische IP-Bereiche vor die Definitionen für allgemeinen Zugriff setzen (bei gleicher Community).

  Weitere Informationen hierzu, insbesondere auch zu der Syntax von **subnet** und **netmask** entnehmen Sie den manpages zu **snmpd.conf**.

- Der Community-Name ist in obigem Beispiel **public**.

  Falls Sie sich aus Sicherheitsgründen für einen anderen Community-Namen entscheiden, so ersetzen Sie den Community-Namen **public** der Beispielkonfiguration durch den von Ihnen gewählten Namen.

  Sie dürfen nicht vergessen, auch an der Management-Station auf der Registerkarte **Network/Snmp** im Eigenschaftsfenster **Server Properties** diesen neuen Community-Namen anzugeben.

- Zugriffe über SNMP, die Werte verändern, sind standardmäßig nicht zugelassen. Wenn Sie der Management-Station erlauben wollen, Werte auf dem verwalteten Server zu ändern bzw. einen Shutdown durchzuführen, dann müssen Sie SNMP **SetRequests** zulassen. Ändern Sie hierzu die letzte Zeile der oben dargestellten Beispielkonfiguration auf:

```
access svGroup "" any noauth exact svView svView none
```

  Außerdem müssen Sie darauf achten, dass die Werte für **AgentPermission** und **AgentShut** auf **3** gesetzt sind. Weitere Informationen zur Definition

dieser Werte in der Datei **config** finden Sie unter "Agenten konfigurieren" auf Seite 53.

- Legen Sie die Zieladresse für SNMP-Traps fest. Tragen Sie hierzu für **trapsink** die IP-Adresse oder den Namen der Management-Station ein. Sie können auch mehrere Management-Stationen eintragen. Für jede Management-Station tragen Sie eine Zeile in die **snmpd.conf** ein:

  ```
  trapsink <host> <community name>
  ```

  Für **<community name>** geben Sie public oder den entsprechenden Community-Namen an, falls Sie einen anderen Namen verwenden.
- Der GAM-Agent für LSI/Mylex RAID Controller kommuniziert über das SMUX-Protokoll (SNMP Multiplex Protokoll) mit dem SNMP Master-Agenten.

  Wenn der GAM-Agent installiert ist, müssen Sie folgende Zeile in die SNMP-Konfigurationsdatei aufnehmen:

  ```
  smuxpeer .1.3.6.1.4.1.1608 mylex
  ```
- Wenn Sie Änderungen vorgenommen haben, starten Sie den Dienst **snmpd** oder den Server neu.

Wenn auf Ihrem Server ein Firewall aktiviert ist, müssen Sie sicherstellen, dass die SNMP-Ports geöffnet sind. Es sollten akzeptiert werden:

- eingehende Pakete auf Port 161 (Service-Name **snmp**) für das Protokolle **udp**,
- herausgehende Pakete auf Port 162 (Service-Name **snmptrap**) für das Protokoll **udp**, damit Traps gesendet werden können.
- Port 3172 (Remote Connector Service) und Port 3173 (ServerView RAID Manager) für das Protokoll **tcp**.
- CIM-Server-Ports 5988 (für HTTP) oder 5989 (für HTTPS)

2.5 Hardware-Uhr (CMOS-Uhr) einstellen

Die CMOS-Uhr muss auf die lokale Zeit eingestellt sein, nicht auf Greenwich-Zeit. Andernfalls startet der automatische Power ON/Power OFF nicht zu der konfigurierten Zeit.

Die lokale Zeit wird auf den verschiedenen Betriebssystemplattformen wie folgt eingestellt:

- SUSE:

  Weisen Sie über **YaST** – **System** der CMOS-Uhr die lokale Zeit zu.

  Für SUSE SLES 11:

  Beachten Sie folgende Vorgabe:

  Die Option **Hardware Clock Set To UTC** muss deaktiviert sein.

  Wählen Sie im Fenster **Date and Time** aus der Auswahlliste **Hardware Clock Set To** auf den Eintrag **Local Time**.

- Red Hat:

  Weisen Sie der CMOS-Uhr über **linuxconf** die lokale Zeit zu:

  Beachten Sie folgende Vorgabe:

  Im Fenster **Date and Time Properties** können Sie auf der Registerkarte **Time Zone** die Option **System Clock** verwenden.

  Die Option **System Clock uses UTC** muss deaktiviert sein.

  Wählen Sie **System** – **Administration** – **Date & Time**.

Mit dem Kommando **date** lassen Sie sich die Systemzeit ausgeben, mit **hwclock --show** die CMOS-Zeit. Verwenden Sie bei abweichenden Zeiten das Kommando **hwclock**, um die CMOS-Zeit an die Systemzeit anzupassen. Weitere Informationen zum Kommando **hwclock** finden Sie unter **hwclock – help**.

2.6 Für die Treiber Monitor-Funktion erforderliche Einstellungen

2.6.1 Treiber Monitor-Funktion auf SLES10 und SLES11

Für Treiber Monitor-Funktion auf SLES10 und SLES11 ist es notwendig, die Konfigurationsdatei **syslog-ng** zu erweitern.

- Für SUSE SLES 10:
  1. Fügen Sie die folgenden Zeilen in die Datei **/etc/syslog-ng/syslog-ng.conf.in** ein:

     ```
     destination hwlog { pipe("/dev/HWLog/syslog_
     fifo"); };
     log { source(src); destination(hwlog); };
     ```

  2. Anschließend führen Sie folgendes Kommando aus:

     ```
     /sbin/SuSEconfig
     ```

- Für SUSE SLES 11:
  1. Fügen Sie die folgenden Zeilen in die Datei **/etc/syslog-ng/syslog-ng.conf** ein:

     ```
     destination hwlog { pipe("/dev/HWLog/syslog_
     fifo"); };
     log { source(src); destination(hwlog); };
     ```

- SUSE SLES 10 und SUSE SLES 11:
  1. Starten Sie YaST und wählen Sie **Novell AppArmor** – **Edit Profile**.
  2. Wählen Sie den Namen des aktiven syslog-Dämons (**/sbin/syslog-ng** oder **/sbin/syslogd**) und klicken Sie **Next**.
  3. Geben Sie im Feld **Enter** oder **modify Filename** den Pfad **/dev/HWLog/syslog_fifo** ein.
  4. Unter **Permissions** aktivieren Sie die Option **Read and Write**.
  5. Speichern Sie diesen Eintrag.
  6. Starten Sie AppArmor neu:

```
/etc/init.d/boot.apparmor restart
```

7. Starten Sie die Syslog-Dienste neu:
   ```
   /etc/init.d/syslog restart
   ```

2.6.2 Treiber Monitor-Funktion unter Red Hat

Für die Treiber Monitor-Funktion unter Red Hat gilt Folgendes:

Während der Installation wird die folgende Zeile in die Konfigurationsdatei des **syslog**-Dämons eingefügt und der **syslog**-Dämon wird neu gestartet:

```
*.info;mail.none;news.none;authpriv.none;cron.none
|/opt/fujitsu/ServerViewSuite/HWLog/path/syslog_fifo
```

Während der Deinstallation wird dieser Eintrag entfernt und der **syslog**-Dämon wird neu gestartet.

Unter Red Hat kann der syslog-Dämon **syslog** (Red Hat5) oder **rsyslog** (Red Hat5.6, Red Hat6) installiert sein.

Unter Red Hat kann der syslog-Dämon **syslog** (Red Hat5) oder **rsyslog** (Red Hat5.6, Red Hat6) installiert sein.

Die Prozedur zur Änderung der **syslog**-Konfigurationsdatei versucht zuerst die **rsyslog**-Datei zu ändern und diesen Dämon neu zu starten. Wenn der **syslog** Dämon eingesetzt wird, darf **rsyslog** nicht installiert sein!

Die Prozedur zur Änderung der **syslog**-Konfigurationsdatei versucht zuerst die **rsyslog**-Datei zu ändern und diesen Dämon neu zu starten. Wenn der **syslog** Dämon eingesetzt wird, darf **rsyslog** nicht installiert sein!

2.7 Kernelmodule für ServerView-Agenten installieren

Bei einigen PRIMERGY-Server-Typen sind Kernelmodule für eine vollständige ServerView-Agenten-Funktion erforderlich. In diesem Abschnitt wird die Installation dieser Kernelmodule für SLES und RHEL beschrieben.

2.7.1 Kernelmodule für ServerView-Agenten installieren (SUSE Linux)

Detaillierte Informationen zum Partner Linux Driver Process (PLDP) für PRIMERGY-Server finden Sie unter: http://ts.fujitsu.com/products/standard_servers/linux_readmes_popup.html

2.7.1.1 Das Treiberkit-Image srvmagt-modules-<version>.iso abrufen

Für das Abrufen des **srvmagt-modules-<version>.iso**-Disk-Image haben Sie folgende Optionen:

- Von der ServerView Suite DVD 2: Wählen Sie **SVSLinux** - **Novell-KMP** und klicken Sie dann der Reihe nach durch die Ordner, die Ihre bevorzugte SLES-Version und das Service-Pack enthalten.
- Von ftp://ftp.ts.fujitsu.com/images/serverview können Sie das DVD-ISO-Image **UPD_LINUX_<version>.iso** herunterladen. Wählen Sie **Novell-KMP** und klicken Sie dann der Reihe nach durch die Ordner, die Ihre bevorzugte SLES-Version und das Service Pack enthalten.
- Von der Website **Driver & Downloads** (http://ts.fujitsu.com/support/downloads.html): Über eine Schnellsuche nach "PLDP svrmagt-modules" im Feld **Driver Quicksearch** wird eine Liste aller verfügbaren PLDP-Treiber-Paket-srvmagt-Module angezeigt, aus der Sie ein entsprechendes Paket auswählen können.

Alternativ können Sie folgendermaßen vorgehen:

a. Wählen Sie **Software** - **ServerView** - **Operation** - **Agents and Providers**, um die Seite **Downloads for Agents and Providers** aufzurufen.

b. Wählen Sie die Seite mit Ihrer bevorzugten SUSE Linux-Version aus.

c. Wählen Sie **Server Management Software** - **ServerView Agents & CIM Providers** aus. Das Disk Image befindet sich im Paket **PLDP driver package srvmagt-modules <version> for SLES<nn> SP<n>** (Dateiname: **FTS_ PLDPdriverpackagesrvmagtmodules<version>.zip**).

2.7.1.2 Das Treiberkit-Image srvmagt-modules-<version>.iso auf dem verwalteten Server bereitstellen

Gehen Sie folgendermaßen vor, um die heruntergeladenen Pakete auf dem verwalteten Server bereitzustellen:

1. Mounten Sie das ISO-Image per Loopdevice und geben Sie das Repository für das System an:

```
# mount -o loop /tmp/srvagt-modules-*.iso /mnt/img
# zypper ar /mnt/img srvmagt
```

2. Installieren Sie das Modul:

```
# zypper install primergy-smbus-kmp-$KERNEL_FLAVOR
```

$KERNEL_FLAVOR ist je nach installiertem Kernel "default" oder "xen".

Wenn Sie nach dem Paket-Signierungsschlüssel mit dem Fingerabdruck A6E12DAE581F5A2C016C58E45FE63BCE79444536 gefragt werden, vertrauen Sie dem Schlüssel.

3. Deaktivieren Sie das Repository wieder:

```
# zypper rr srvmagt
# umount /mnt/img
```

2.7.1.3 Kernelmodule aus einem Online-Repository abrufen

Alternativ können Sie Ihr System für einen Zugriff auf die Fujitsu-Treiberpaket-Repositorys über http://patches.ts.fujitsu.com/linux/index_pldp.html (oder über eine Spiegelung, wenn Ihr System keinen direkten Internetzugang hat) konfigurieren.

In diesem Fall müssen Sie die ISO-Datei nicht herunterladen.

Gehen Sie wie folgt vor:

1. Geben Sie bei Bedarf das Treiber-Repository an:

   Bevor Sie das folgende Kommando senden, müssen Sie die Betriebssystemversion an Ihre Anforderungen anpassen.

   ```
   # zypper ar
   http://patches.ts.fujitsu.com/linux/pldp/SLE11/sles
   11-sp3 primergy-sles11-sp3
   ```

2. Installieren Sie das Modul:

   ```
   # zypper install primergy-smbus-kmp-$KERNEL_FLAVOR
   ```

2.7.2 Kernelmodule für ServerView-Agenten installieren (Red Hat Linux)

Weitere Informationen zum Red Hat Driver Update Process (RHDUP) für PRIMERGY-Server finden Sie unter: http://ts.fujitsu.com/products/standard_servers/linux_readmes_popup.html

2.7.2.1 Das Treiber-Disk-Image srvmagt-modules-<version>.iso abrufen

Für das Abrufen des **srvmagt-modules-<version>.iso**-Disk-Image haben Sie folgende Optionen:

- Von der ServerView Suite DVD 2: Wählen Sie **SVSLinux** - **RHDUP** und klicken Sie dann der Reihe nach durch die Ordner, die Ihre bevorzugte RHEL-Version und das Versions-Update enthalten.
- Von ftp://ftp.ts.fujitsu.com/images/serverview können Sie das DVD-ISO-Image **UPD_LINUX_<version>.iso** herunterladen. Wählen Sie **RHDUP** und

klicken Sie dann der Reihe nach durch die Ordner, die Ihre bevorzugte RHEL-Version und das Versions-Update enthalten.

- Von der Website **Driver & Downloads** (http://ts.fujitsu.com/support/downloads.html): Über eine Schnellsuche nach "RHDUP svrmagt-modules" im Feld **Driver Quicksearch** wird eine Liste aller verfügbaren RHDUP-Treiberpaket-srvmagt-Module angezeigt, aus der Sie ein entsprechendes Paket auswählen können.

  Alternativ können Sie folgendermaßen vorgehen:

  a. Wählen Sie **Software** - **ServerView** - **Operation** - **Agents and Providers**, um die Seite **Downloads for Agents and Providers** aufzurufen.

  b. Wählen Sie die bevorzugte Red Hat Linux-Version aus.

  c. Wählen Sie **Server Management Software** - **ServerView Agents & CIM Providers** aus. Das Disk Image befindet sich im Paket "RHDUP driver package srvmagt-modules <version> for SLES<nn> SP<n>" mit dem Dateinamen **FTS_ RHDUPdriverpackagesrvmagtmodules<version>.zip**.

2.7.2.2 Das Treiber-Disk-Image srvmagt-modules-<version>.iso auf dem verwalteten Server bereitstellen

Gehen Sie folgendermaßen vor, um die heruntergeladenen Pakete auf dem verwalteten Server bereitzustellen:

1. Mounten Sie das ISO-Image per Loopdevice und geben Sie das Repository für das System an:

   ```
   # mount -o loop /tmp/srvmagt-modules-*.iso /mnt/img
   # cp /mnt/img/dud.repo
   /etc/yum.repos.d/srvmagt.repo
   ```

2. Legen Sie den Pfad zum Mount Point in der **.repo**-Datei fest:

   Dieser Schritt ist nur erforderlich, wenn **primergy-dup** noch nie auf dem System installiert wurde.

   ```
   # sed -i 's,<mount point>,mnt/img,'\
   /etc/yum.repos.d/srvmagt.repo
   ```

3. Installieren Sie primergy-dup mit dem GPG-Schlüssel:

```
# yum install --nogpgcheck primergy-dup
```

Wenn Sie nach dem Paket-Signierungsschlüssel mit dem Fingerabdruck A6E12DAE581F5A2C016C58E45FE63BCE79444536 gefragt werden, vertrauen Sie dem Schlüssel.

4. Kommentieren Sie den GPG-Schlüsselkommentar aus dem **primergy-dup**-Paket in der **.repo**-Datei aus:

Dieser Schritt ist nur erforderlich, wenn **primergy-dup** noch nie auf dem System installiert wurde.

```
# sed -i '/gpgkey=file.*/s/^# //'
/etc/yum.repos.d/srvmagt.repo
```

5. Installieren Sie die Module:

```
# yum install kmod-smbus
# umount /mnt/img
```

Wenn Sie gebeten werden, den Treiber-Signierungsschlüssel 0x79444536 zu bestätigen, stimmen Sie zu.

6. Deaktivieren Sie das Repository wieder:

```
# sed -i '/enabled/s/=yes/=no/'
/etc/yum.repos.d/srvmagt.repo
```

2.7.2.3 Kernelmodule aus einem Online-Repository abrufen

Alternativ können Sie Ihr System für einen Zugriff auf die Fujitsu-Treiberpaket-Repositorys über http://patches.ts.fujitsu.com/linux/index_pldp.html (oder über eine Spiegelung, wenn Ihr System keinen direkten Internetzugang hat) konfigurieren.

In diesem Fall müssen Sie die ISO-Datei nicht herunterladen.

Gehen Sie wie folgt vor:

1. Geben Sie bei Bedarf das Repository an:

```
# cd /etc/yum.repos.d
```

Bevor Sie das folgende Kommando senden, müssen Sie die Betriebssystemversion an Ihre Anforderungen anpassen.

```
# curl -o primergy-rhel6-u4.repo
http://patches.ts.fujitsu.com/linux/pldp//RHEL6/rhe
l6-u4.repo
```

2. Geben Sie bei Bedarf den Fujitsu GPG-Schlüssel an:

   ```
   # yum install --nogpgcheck primergy-dup
   ```

3. Installieren Sie die Module:

   ```
   # yum install kmod-smbus
   ```

Wenn Sie gebeten werden, den Treiber-Signierungsschlüssel 0x79444536 zu bestätigen, stimmen Sie zu.

3 Installation der ServerView-Agenten

Bei Verwendung einer Public Key-Infrastruktur (PKI) zur Client-Authentifzierung:

Client-Authentifizierung schützt den verwalteten Server sowohl vor dem Zugriff einer nicht vertrauenswürdigen Management-Station als auch vor dem Zugriff einer nicht-privilegierten Anwendung, die auf der Management-Station läuft. Sie können die Zertifikatsdateien entweder gleich zu Beginn mit den ServerView-Agenten installieren oder auf einem verwalteten Server, auf dem die ServerView-Agenten bereits installiert sind.

Bei der Installation der Zertifikatsdateien mit den ServerView-Agenten müssen die Zertifikatsdateien bereits vor den Agenten auf dem verwalteten Server installiert sein.

Nähere Informationen finden Sie im Handbuch "Benutzerverwaltung in ServerView".

Eine Übersicht der zusätzlich benötigten Pakete für den ServerView Operations Manager und ServerView RAID Manager finden Sie im Handbuch „Installation unter Linux“.

Die Installation von ServerView-Agenten unter Citrix XenServer wird über die XenServer Supplement CD ermöglicht. Der CD-Inhalt befindet sich auf der ServerView Suite DVD 2 (**ServerView – XenServer Supplements** oder **SVSSoftware\Software\XenServer-Supplements**).
Sie können das ISO-Abbild auch vom Fujitsu Technology Solutions Web-Server herunterladen (http://support.ts.fujitsu.com/download/).
Es enthält die erforderlichen Software-Pakete, Skripte zur Unterstützung der Installation sowie Konfigurationsdokumentation und Versionshinweise.

3.1 Voraussetzungen

Bevor die ServerView-Agenten installiert werden, müssen mehrere Voraussetzungen erfüllt sein:

- Die relevanten **Net-SNMP**-Pakete müssen gemäß der Betriebssystemplattform installiert sein:

SUSE SLES	**net-snmp**
Red Hat Enterprise Linux	**net-snmp** und **net-snmp-utils**
Oracle Linux	**net-snmp** and **net-snmp-utils**
Citrix XenServer	**net-snmp**

- Für die ServerView-Agenten werden folgende Software-Pakete benötigt:

  Diese Pakete können mit **YaST / YUM** (empfohlen) installiert werden.

  - SUSE SLES (die Benennung des Pakets hängt von der SLES-Version und der Architektur ab):

SLES V11	**libstdc++33, libcurl4** und **libopenssl0_9_8**
SLES 12	**libstdc++6**, **libcurl4**,**libopenssl1_0_0**

  - Red Hat, Oracle Linux, Citrix XenServer:

RHEL5	Linux-Agenten sind immer noch 32-Bit-Anwendungen, deshalb werden 32-Bit-Pakete auch in der 64-Bit-Architektur benötigt. **openssl.i686** **compat-libstdc++-33.i386** **curl.i386**

RHEL6/OL6	**openssl** **compat-libstdc++-33** **libcurl**
RHEL7/OL7	**openssl** **llibstdc++** **libcurl**
Citrix XenServer	**openssl** **compat-libstdc++-33**

- Zusätzliche Voraussetzungen für den ServerView System Monitor:
  - Ein grafisches Desktop-Environment basierend auf X11. Unterstützt werden KDE und GNOME.
  - Nur für den lokalen ServerView System Monitor: Ein geeignetes Java Runtime Environment >= V1.6.0_25. Am besten verwenden Sie das Java Runtime Environment von der ServerView Suite DVD 2. Für eine Umgebung in japanischer Sprache muss eine Java-Laufzeitumgebung >= V1.6.0_30 verwendet werden.
  - Nur für den lokalen ServerView System Monitor: Bitte stellen Sie auch sicher, dass Sie auf 64-Bit-Maschinen die 64-Bit-Java Runtime-Version verwenden.
  - Um RAID-Information anzeigen zu können, muss der ServerView RAID Manager installiert sein und laufen.
  - Um die Online-Hilfe anzeigen zu können, muss ein Web-Browser installiert sein.
- Zusätzliche Voraussetzungen für ServerView CIM-Provider:
  - ServerView CIM-Provider sind 64-Bit-binär und arbeiten deshalb nur auf x86-64-Architekturen.
  - Ein CIMOM-Service (CIM Object Manager) muss verfügbar sein. Unterstützte CIMOMs sind SFCB und OpenPegasus.
- Für das Management Ihrer RAID-Peripherie müssen Sie auf Ihrem System zusätzlich den ServerView RAID Manager installieren. Die Installation ist im Benutzerhandbuch "RAID Management" beschrieben.

- Mounten Sie die ServerView Suite DVD 2 und öffnen Sie im Root-Verzeichnis der DVD die Datei **start.html** im Web-Browser. Wechseln Sie zu **ServerView – Agents and Providers** und klicken Sie in der Tabelle auf den Verweis **ServerView Agents Linux and VMware**.

  Die Liste der unterstützten PRIMERGY Server finden Sie unter **Unterstützte Systeme**.
- Die SELinux-Funktion muss deaktiviert sein (nicht erforderlich bei Red Hat ab Version 6.0).

3.2 Skript-basierte Installation

Die Installation des ServerView-Agenten erfolgt über das Skript **srvmagt**. Dieses testet und überprüft alle bereits bekannten Abhängigkeiten, trifft sämtliche erforderlichen Vorbereitungen und führt schließlich die nötigen Aktionen durch, um ServerView-Agenten für Linux auf dem System einzurichten.

Das Skript führt folgendes aus:

- Erkennung der Linux Distribution (z.B. SUSE, Red Hat)
- Erkennung der Kernel-Version und Architektur (x86, x86-64 oder ia64)
- Erkennung des PRIMERGY Server Modells anhand der BIOS Daten.
- Erkennung, ob PLDP (Partner Linux Driver Process) und DUP (Driver Update Process) unterstützt werden. In diesem Fall versucht das Skript automatisch die ServerView Kernelmodule (KMP), falls erforderlich, zu installieren.
- Überprüfung, ob das entsprechende SNMP-Paket und andere Modell-abhängige Pakete bzw. Distributionen vorhanden sind.
- Einstellungen in der Datei **snmpf.conf** (nur bei japanischer Betriebssystemumgebung)

  Wenn Sie ServerView-Agenten auf einem japanischem Betriebssystem installieren, überprüft das Installations-Skript, ob der SNMP-Dienst konfiguriert werden muss. Wenn dem so ist, wird die Backup-Datei **/etc/snmp/snmpd.conf_svsave** erzeugt und die folgenden Einträge werden in die Datei **/etc/snmp/snmpd.conf** eingetragen.

  ```
  com2sec svSec localhost public
  com2sec svSec 127.0.0.1 public
  ```

```
com2sec svSec default public
group svGroup v1 svSec
view svGroup included .1
access svGroup "" any noauth exact svView svView
none
trapsink 127.0.0.1
```

Weitere Informationen finden Sie unter "SNMP-Dienste konfigurieren" auf Seite 30.

3.2.1 Installation über die ServerView Suite DVD 2

Die ServerView Suite DVD 2 enthält die RPM-Pakete zur Installation der ServerView-Agenten und das Shell Archiv **srvmagtDVD.sh**. Das Skript finden Sie auf der ServerView Suite DVD 2 im folgenden Verzeichnis:

SVSSoftware – Software – ServerView – Linux – Agents

Zur Agenten-Installation gehen Sie wie folgt vor:

1. Legen Sie die ServerView Suite DVD 2 ein und, falls erforderlich, mounten Sie die DVD.
2. Öffnen Sie (als root) ein Terminal.
3. Wechseln Sie in das Verzeichnis

   SVSSoftware – Software – ServerView – Linux – Agents
4. Geben Sie das folgende Kommando ein:

   ```
   sh srvmagtDVD.sh [-R] [--ssm install | not-install]
   ```

   -R

   Installiert das Paket für den ServerView RAID Manager, wenn es mit den anderen RPM-Paketen ausgeliefert wurde.

   --ssm install | not-install

   Legt die Installation des lokalen ServerView System Monitor und der ServerView System Monitor Web-Oberfläche fest. Mit der Standardeinstellung werden beide Pakete installiert.

   Diese Option wird nur bei Red Hat-, SUSE- und Oracle-Linux-Systemen ausgewertet.

Das Skript führt die Installation dann automatisch aus.

Falls die Installation von ServerView System Monitor oder CIM fehlschlägt, wird die Installation der ServerView-Agenten nicht abgebrochen.

3.2.2 Installation von einem Verzeichnis

Sie können die ZIP-Datei, die das Shell-Archiv **srvmagt.sh** und die RPM-Pakete der ServerView-Agenten enthält, vom Fujitsu Technology Solutions Web-Server in ein beliebiges Verzeichnis herunterladen.

Wichtiger Hinweis:

Für das nachfolgend beschriebene Verfahren ist es erforderlich, dass das Treiberkit/die Treiber-Disk **srvmagt-modules-<version>.iso** bereits auf dem verwalteten Server gemountet wurde (siehe Abschnitt "Kernelmodule für ServerView-Agenten installieren (SUSE Linux)" auf Seite 36 und "Kernelmodule für ServerView-Agenten installieren (Red Hat Linux)" auf Seite 38

Zur Agenten-Installation gehen Sie wie folgt vor:

1. Laden Sie das entsprechende **ServerView Agents Linux**-Paket (**FTS_ ServerViewAgentsLinux_<version>_<nnnnnnn>.zip** wie nachfolgend beschrieben herunter:
   a. Wählen Sie auf der Seite **Driver & Downloads** (http://ts.fujitsu.com/support/downloads.html) **Software** - **ServerView** - **Operation** - **Agents and Providers**, um die Seite **Downloads for Agents and Providers** aufzurufen.
   b. Wählen Sie die bevorzugte Red Hat /SUSE Linux-Version aus.
   c. Wählen Sie **Server Management Software** - **ServerView Agents & CIM Providers**- **SeverView Agents for Linux**.
2. Speichern Sie die RPM-Pakete und das Shell Archiv **srvmagt.sh** in ein beliebiges Verzeichnis.
3. Öffnen Sie (als root) ein Terminal.
4. Wechseln Sie in das entsprechende Verzeichnis:

```
cd <path>
```

5. Gewähren Sie die Berechtigung, **srvmagt.sh** auszuführen:
   ```
   chmod +x srvmagt.sh
   ```

6. Geben Sie das folgende Kommando ein:
   ```
   ./sh srvmagt.sh [optioninstall
   ```
   Die Optionen werden in "Das Skript srvmagt" auf Seite 50 beschrieben.

Das Skript installiert die RPM-Pakete.

3.3 Installation mit dem rpm-Kommando

Bei der Installation mit dem Kommando **rpm** gehen Sie folgendermaßen vor:

1. Starten Sie (als root) ein Terminal.
2. Mounten Sie die ServerView Suite DVD 2.
3. Wechseln Sie in das Verzeichnis, in dem die Linux-Agenten sind:
   ```
   cd /mnt/cdrom/SVSSoftware/
   Software/ServerView/Linux/Agents
   ```
4. Installieren Sie die folgenden RPM-Pakete:
   ```
   rpm -U ServerViewConnectorService-<scs-version>-
   <release>.<arch>.rpm
   rpm -U srvmagt-mods_src-<Version>-
   <release>.<arch>.rpm
   rpm -U srvmagt-eecd-<Version>-<release>.<arch>.rpm
   rpm -U srvmagt-agents-<Version>-
   <release>.<arch>.rpm
   rpm -U srv-cimprovider-<version>.x86_64.rpm
   rpm -U SVSystemMonitor-<Version>.noarch.rpm
   rpm -U SSMWebUI-<Version>.noarch.rpm
   ```

Die Pakete müssen in der oben genannten Reihenfolge installiert werden.

Das Paket **srv-cimprovider-<version>.x86_64.rpm** kann nur in einer x86-64 Linux-Umgebung installiert werden.

<scs-version>
Geben Sie die Version und die Release-Nummer von Remote Connector Service an (z. B. 2.10.02).

<Version>
Geben Sie die Version und die Release-Nummer des ServerView Linux-Agenten an (z. B. 7.10-06).

<arch>
Geben Sie die Architektur der Pakete an: 32 Bit oder 64 Bit.

3.4 Mögliche Fehlerquellen

- Falls bei der Compilierung Fehler auftreten, dann kann das daran liegen, dass der passende Quellcode des Kernels nicht auf dem Server vorhanden ist.
- Wenn Sie die Compilierung der Module nachträglich per Hand starten wollen, können Sie dies mit dem folgenden Befehl machen:

  ```
  /etc/init.d/eecd_mods_src start
  ```

  Falls Sie die Ausgaben des Compilers angezeigt bekommen wollen, starten Sie make direkt im Verzeichnis **/etc/srvmagt/sources**.

3.5 ServerView-Agenten Maintenance nach der Installation

3.5.1 Das Skript srvmagt

Nachdem Sie die ServerView-Agenten für Linux installiert haben, wie beschrieben unter "Installation über die ServerView Suite DVD 2" auf Seite 47

oder unter "Installation von einem Verzeichnis" auf Seite 48, werden über das Skript **srvmagt** weitere Funktionen bereitgestellt.

1. Öffnen Sie (als root) ein Terminal.
2. Geben Sie das Kommando ein, siehe Syntax.

Syntax

```
[/usr/sbin/]srvmagt [option] [action]
```

Für **option** können Sie angeben:

-f

Erzwingt die ausgewählte Aktion unabhängig von ausgegebenen Warnungen/Ablehnungen.

In diesem Fall handeln Sie auf eigenes Risiko und Verantwortung. Das Verhalten und die Funktion ist undefiniert.

-h | --help

Gibt die Kommandosyntax aus und beendet das Kommando.

-n

Während der Installation mit der install-Aktion werden keine ServerView-Agenten-Daemone gestartet.

-p <path>

Das Verzeichnis mit den RPM-Paketen kann angegeben werden.

path ist die Pfadangabe zu einem lokalen oder fernen Dateisystem.

Die Pfadangabe darf keine Leerzeichen oder Sonderzeichen enthalten.

-R

Installiert das Paket für den ServerView RAID Manager, wenn es mit den anderen RPM-Paketen ausgeliefert wurde.

--ssm install | not-install

Legt die Installation des lokalen ServerView System Monitor und der ServerView System Monitor Web-Oberfläche fest. Mit der Standardeinstellung werden beide Pakete installiert.

Diese Option wird nur bei Red Hat-, SUSE- und Oracle-Linux-Systemen ausgewertet.

-v <vers>
Angabe der Skriptversion. Standardmäßig die Version des Skripts.

--version
Druckt die Version des Skripts und beendet das Kommando.

-V
Druckt ausführliche Informationen.

Für **action** können Sie angeben:

install
Installiert (repariert, aktualisiert) alle RPM-Pakete des ServerView-Agenten für Linux entsprechend der bereits installierten Konfiguration und der Version die über die Option **-v** angegeben wird. Die entsprechenden Dienste werden anschließend gestartet, außer die Option **-n** wurde angegeben.

start
Startet den ServerView-Agenten für Linux.

restart
Startet den ServerView-Agenten für Linux neu.

Status
Zeigt den Status des ServerView-Agenten für Linux.

diag
Sammelt Diagnoseinformation über den Aufruf PrimeCollect(8).

stop
Stoppt den ServerView-Agenten für Linux.

remove
Entfernt alle RPM-Pakete des ServerView-Agenten für Linux.

Bei Verwendung des Betriebssystems Citrix XenServer wird gleichzeitig auch das ServerView RAID-Paket entfernt.

3.5.2 Agenten konfigurieren

Die Datei **/etc/srvmagt/config** enthält Informationen, mit denen Sie den Zugriff auf das verwaltete System beschränken und andere Betriebsparameter auswählen können.

Zeilen, die mit einem „#" beginnen, sind Kommentarzeilen, die anderen Zeilen haben das Format:

```
<schlüsselwort>=<wert>
```

AgentPermission	Prinzipielle Erlaubnis für andere Systeme, Werte auf dem lokalen Server mit Hilfe von SNMP-Kommandos zu setzen (2: nicht erlaubt, 3: erlaubt, Voreinstellung: 2 (Voreinstellung bei japanischer Betriebssystemumgebung: 3)). Falls Sie diese SNMP SetRequests zulassen wollen, müssen Sie hier den Wert auf 3 setzen sowie die SNMP-Dienste entsprechend konfigurieren (siehe "SNMP-Dienste konfigurieren" auf Seite 30).
AgentShut	Erlaubnis für andere Systeme, einen Shutdown/Reboot auf dem lokalen Server mit SNMP-Kommandos durchzuführen (2: nicht erlaubt, 3: erlaubt, Voreinstellung: 2 (Voreinstellung bei japanischer Betriebssystemumgebung: 3)). Falls Sie diese SNMP SetRequests zulassen wollen, müssen Sie hier den Wert auf **3** setzen sowie die SNMP-Dienste entsprechend konfigurieren (siehe "SNMP-Dienste konfigurieren" auf Seite 30).
ShutdownDelay	Legt die Zeitspanne (in Minuten) zwischen einem SNMP-Shutdown-Request und dem Shutdown fest.

NoAccountCheck	Wird hierfür ein anderer Wert als 0 festgelegt, so wird kein Passwort abgefragt, wenn über den Operations Manager Einstellungen verändert werden. Die Standard-Einstellung ist 0, d.h. standardmäßig ist die Benutzerauthentifizierung eingeschaltet. In diesem Fall muss unter **UserGroup** eine Benutzergruppe angegeben sein, der der Benutzer angehören muss, der SET-Operationen durchführen können soll. Beachten Sie, dass eine deaktivierte Passwortabfrage ein erhebliches Sicherheitsrisiko darstellen kann.
UserGroup	Falls bei **NoAccountCheck** 0 angegeben wurde, benötigt der Operations Manager an der Management-Station eine Benutzer/Passwort-Kombination, um SNMP-Einstellungen verändern zu können. Der Benutzer muss, um Zugriffsberechtigung zu erhalten, derjenigen Gruppe angehören, die unter **UserGroup** festgelegt ist. Die Standardeinstellung ist **bin**, zu der auch **root** gehört. (Die Voreinstellung bei japanischer Betriebssystemumgebung ist **svagtuser**.) Falls die hier angegebene Benutzergruppe noch nicht existiert, so muss sie nachträglich noch mit betriebssystemspezifischen Mitteln angelegt werden.
ScanTapeDevices	Wird hierfür ein anderer Wert als 0 festgelegt, werden die Gerätedateien **/dev/nst*** für Magnetbandlaufwerke eröffnet, um deren aktuellen Status zu ermitteln. Diese Eröffnung kann (abhängig vom Treiber) einen unbeabsichtigten Wechsel der Lese-/Schreibposition des Bandes auslösen. Falls das Band von mehreren Servern zugleich verwendet wird, stellt dieser Parameter sicher, dass der Operations Manager laufende Bandoperationen (z. B. Datensicherung) nicht durch Zustandsabfragen stört. Die Standardeinstellung ist 0, d.h. Bandgerätedateien werden nicht eröffnet.

TraceFileLimit	Steuert die Größe der unter **/var/log/srvmagt** abgelegten Trace-Dateien (1 ist der Standard-Wert, benötigter Platz ca. 200 MB, 0 bedeutet keine Trace Dateien, 2 bedeutet extra große Trace-Dateien ca. 400 MB).
InventoryRescan	Legt die Zeitspanne (in Minuten) fest, in der die Inventory Daten des Servers aktualisiert werden. Unterstützte Werte sind 0, 120 bis 34560. Der Wert 0 deaktiviert die Aktualisierung. Werte zwischen 1 und 120 werden auf 120 gesetzt. Werte größer als 34560 werden auf 0 gesetzt. Der Standardwert ist 120. (Voreinstellung bei japanischer Betriebssystemumgebung ist 0).

Eine Änderung der Datei **config** wird erst nach einem Neustart des Agenten wirksam. Dazu starten Sie den Server neu oder geben folgendes Kommando als Systemverwalter ein:

```
/usr/sbin/srvmagt restart
```

Citrix Xen oder Xen

Um den Performance und Threshold Manager für Citrix Xen oder Xen im ServerView Operations Manager zu unterstützen, ist es notwendig, Informationen zum Benutzerkonto für das VMware ESX System über den ServerView VME Agent zu konfigurieren. Gehen Sie dazu wie folgt vor:

1. Bearbeiten Sie die Datei **/etc/srvmagt/VME/etc/app.config.xml**.
2. Suchen Sie nach dem Abschnitt **<authentication>**.
3. Tragen Sie die notwendigen Benutzer- und Password-Information ein (z. B. **<User>root</User><Password>wheel</Password>**)

   Da das Passwort in Klartext angegeben wird, sollte der Zugriff auf diese Datei begrenzt werden und kein privilegierter Benutzer verwendet werden.
4. Sichern Sie die Datei.
5. Führen Sie einen Neustart der ServerView-Agenten durch.

KVM Server benötigen Benutzername und Passwort nicht.

3.5.3 Verbesserte Verfügbarkeit der ServerView-Agenten

Das Start-Skript **srvmagt(8)** des ServerView-Agenten ruft alle 15 Minuten das srvmagt cron-Skript **srvmagtCron** auf.

srvmagtCron überprüft den Dienst eecd, die ServerView-Agenten, den **SVRemoteConnector** und den SNMP-Dienst **snmpd** und startet sie erneut, falls sie nicht laufen. Das Skript schreibt zusätzlich die Uhrzeit jeder Überprüfung in die erste Zeile der Datei **/var/log/srvmagt/log.srvmagtCron**.

Das Anhalten des ServerView-Agenten mit **srvmagt(8)** bewirkt, dass diese zeitliche Überwachung ausgeschaltet wird.

srvmagtCron wird nicht aus der Root-crontab entfernt um Änderungen in der sensitiven crontab gering zu halten. Die eigentliche Ausführung hängt davon ab, ob die Datei **srvmagtCronOn** im Root-Verzeichnis **srvmagt** angelegt wurde. Diese Datei wird während des Starts der ServerView-Agenten angelegt und wird gelöscht wenn die ServerView-Agenten angehalten werden.

3.5.4 Deinstallation der ServerView-Agenten

Die im BIOS des Servers gespeicherten Elemente werden selbst dann nicht wiederhergestellt, wenn der ServerView-Agent deinstalliert wird. Stellen Sie den ursprünglichen Zustand der Einstellungen wieder her und deinstallieren Sie dann den ServerView-Agenten. Führen Sie vor der Deinstallation des ServerView-Agenten folgende Schritte aus:

1. Deaktivieren Sie die Einstellungen von Software Watchdog, BOOT Watchdog und Power ON/OFF.
2. Wenn eine Schwellwertüberwachung und Berichtserstellung über Performance Manager ausgeführt wurde, beenden Sie diese Dienste auf dem Server.
3. Bei der Deinstallation des ServerView-Agenten werden die Einstellungen gelöscht, die mit ServerView Operations Manager konfiguriert wurden (z. B. die Einstellungen für den Einschaltplan und ASR).

   Es ist keine Option zur automatischen Übernahme der Einstellungen vorhanden. Erstellen Sie deshalb vor der Deinstallation eine Kopie der

Einstellungen. Diese müssen nach der Update-Installation erneut konfiguriert werden.

Geben Sie zur Deinstallation des ServerView-Agenten Folgendes ein:

```
/usr/sbin/srvmagt remove
```

Bei Citrix XenServer wird ServerView RAID Manager ebenfalls über dieses Kommando deinstalliert.

3.5.5 Agenten starten und stoppen

Nach der Installation der Linux-Agenten werden die Agenten automatisch bei einem Systemstart gestartet. Für Diagnosezwecke kann es sinnvoll sein, die Agenten explizit zu stoppen und erneut wieder zu starten.

Agenten starten

Sie starten die Agenten mit folgendem Aufruf:

```
/usr/sbin/srvmagt start
```

Beachten Sie, dass der SNMP Master-Agent **snmpd** gestartet sein muss, bevor Sie die Linux-Agenten starten.

Agenten stoppen

Sie stoppen die Agenten mit folgendem Aufruf:

```
/usr/sbin/srvmagt stop
```

3.5.6 ServerView CIM-Provider starten und stoppen

Das Starten und Stoppen des ServerView CIM-Providers wird durch den CIMOM erledigt.

Wie Sie den CIMOM starten und herunterfahren, finden Sie in der Dokumentation des entsprechenden CIMOM.

3.5.7 Zusätzliche Informationen

- Wenn eine S30 oder S40 an einem Server über SCSI (SAF-TE) angeschlossen ist, aber nicht vom Agenten registriert wird, dann kann es daran liegen, dass

nicht genug Gerätedateien in Linux eingerichtet sind. Diese Gerätedateien sind für die Kommunikation der SNMP-Agenten mit den Speicher-Subsystemen notwendig. Standardmäßig richtet Linux 16 Gerätedateien für SCSI-Anschlüsse ein: **/dev/sg0** bis **/dev/sg15**. Falls Sie mehr als 16 Geräte über SCSI angeschlossen haben, müssen Sie zusätzliche Gerätedateien hinzufügen. Die Anzahl der SCSI-Gerätedateien können Sie der Datei **/proc/scsi/scsi** entnehmen. Zusätzliche Gerätedateien (**/dev/sg**) fügen Sie mit folgendem Kommando hinzu:

```
mknod /dev/sg<number> c 21 <number>
```

Für **<number>** geben Sie Zahlen fortlaufend in Abhängigkeit von dem letzten vorhandenen Eintrag ein (z.B.16 und höher, falls der letzte Eintrag die Nummer 15 enthält). Nach dem Anlegen neuer Gerätedateien müssen Sie den Server neu starten.

- Wenn neue Hardware (z.B. ein Remote Service Board) eingebaut oder neue Speicher-Subsysteme angeschlossen und nicht erkannt werden, dann müssen Sie einen "Rescan" des **eecd** (environment enclosure control daemon) machen. Dazu starten Sie den **eecd** folgendermaßen neu:

```
/etc/init.d/srvmagt stop
/etc/init.d/eecd stop
/etc/init.d/eecd rescan
/etc/init.d/srvmagt start
```

3.5.8 Administrativen Benutzer festlegen

Nur die Benutzer, die der Gruppe mit **Administrator**-Berechtigungen für ServerView angehören, können solche Tätigkeiten durchführen, wie Einstellungen zu Automatic Server Reconfiguration & Restart (ASR) (z.B. für Lüfter, Temperatur, Neustart) für die überwachten Server zu konfigurieren und die Server vom ServerView Operations Manager aus herunterzufahren. Für diese Tätigkeiten werden Name und Passwort des administrativen Benutzers benötigt.

Die Gruppe mit **Administratorrechten** ist eine auf **UserGroup** gesetzte Gruppe, wie beschrieben unter "Agenten konfigurieren" auf Seite 53.

Gehen Sie wie folgt vor, um einen administrativen Benutzer festzulegen.

- Einen neuen Benutzer als administrativen Benutzer erstellen:

  Melden Sie sich als root an und führen Sie folgende Kommandos aus:

  1. Geben Sie den **group name that has Administrator privileges** in der Option **G** des Kommandos **useradd** an:

     ```
     # useradd -G <group name that has Administrator
     privileges> <user name>
     ```

     ```
     # passwd <user name>
     ```

     Für **<user name>** geben Sie einen Namen für den Benutzer an, der erstellt werden soll.
  2. Verwenden Sie das Kommando **passwd**, um ein Passwort für den neuen Benutzer festzulegen. Das Passwort muss zur Bestätigung zweimal eingegeben werden.

  Der neu erstellte Benutzer wird aktiviert, sobald das Passwort festgelegt worden ist. Weitere Informationen zu den einzelnen Kommandos finden Sie in den manpages zu **useradd (8)** und **passwd (1)**.

- Einen vorhandenen Benutzer als administrativen Benutzer festlegen:

  Setzen Sie sich mit dem Systemadministrator in Verbindung, um zu klären, ob der vorhandene Benutzer mehreren Gruppen angehört und führen Sie dann folgendes Kommando aus.

  Wenn der Benutzer nur der Hauptgruppe angehört:

  ```
  # usermod -G <group name that has Administrator
  privileges> <user name>
  ```

  Wenn der Benutzer mehreren Gruppen angehört:

  ```
  # usermod -G <group name that has Administrator
  privileges>,<user group,...> <user name>
  ```

  Geben Sie den group name that has Administrator privileges in der Option **G** des Kommandos **usermod** an. Um mehrere Gruppen festzulegen, trennen Sie diese mit einem Komma ",". Wenn die Gruppe, der der Benutzer vorher angehörte nicht festgelegt wird, wird der Benutzer aus dieser Gruppe gelöscht. Wenn die Gruppe, zu der der Benutzer zuvor gehörte, nicht angegeben ist, wird der Benutzer aus dieser Gruppe gelöscht. Geben Sie alle Gruppen an, zu denen der Benutzer gehören soll.

Für **<user name>** geben Sie den Benutzernamen als administrativen Benutzer an.

Weitere Informationen zum Kommando **usermod** finden Sie in der manpage zu **usermod (8)**.

Sie können die Gruppen auch direkt mit dem Kommando**vigr** oder über Tools auf der grafischen Oberfläche festlegen. Weitere Informationen finden Sie in der manpage zu **vigr (8)** oder in den Handbüchern zu Red Hat Linux.

3.5.9 Geänderte Rechnerinformation nach der Installation

Wenn der Rechnername oder IP-Adresse geändert wird für den Server, auf dem der ServerView Linux-Agent verwaltet und installiert ist, müssen die Einstellungen etc. nicht auf dem ServerView Linux-Agenten geändert werden.

Wenn Sie aber vorher die Datei **snmpd.conf** an Ihre individuelle Umgebung angepasst haben, müssen Sie eventuell die Datei **snmpd.conf** erneut bearbeiten.

Nachdem Sie die Datei **snmpd.conf** bearbeitet haben, starten Sie den Dienst snmpd und den ServerView Linux-Agenten neu:

1. Melden Sie sich als root an.
2. Führen Sie folgende Kommandos aus.

```
# /usr/sbin/srvmagt stop
# /etc/init.d/snmpd stop
# /etc/init.d/snmpd start
# /usr/sbin/srvmagt start
```

3.5.10 Update-Installation / Kernel-Update

Dieser Abschnitt beschreibt den Update-Installationsprozess für den ServerView Linux-Agenten.

1. Wenn Sie den Software-Watchdog und den BOOT-Watchdog mit **Enable** aktiviert haben, deaktivieren Sie diese mit **Disable**.
2. Aktualisieren Sie den Kernel via Kernel-Update und starten Sie dann das Betriebssystem neu.

3. Dateierstellung **/etc/snmp/snmpd.conf_svsave** (nur für Japan).

   Kontrollieren Sie, ob die Datei **/etc/snmp/snmpd.conf_svsave** vorhanden ist.

   Wenn die Datei nicht vorhanden ist, erstellen Sie sie mit dem folgenden Kommando:

   ```
   # cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf_
   svsave
   ```

   Wenn die Datei **snmpd.conf_svsave** vorhanden ist, wird sie nicht vom Installations-Skript bearbeitet.
4. Aktualisieren Sie die ServerView Linux-Agenten.
5. Wenn Sie den Software-Watchdog und den BOOT-Watchdog im Schritt 1 deaktiviert haben, aktivieren Sie diese erneut.

3.5.11 Berichte ausgeben mit dem Performance Manager

Über die Berichteinstellungen im Performance Manager können Berichte ausgegeben werden.

Berichtdaten speichern

Die Berichtdaten werden im folgenden Verzeichnis gespeichert:
/var/srvmagt/reports/

Dateien der Berichtdaten

Die folgenden Dateien werden für jeden Bericht erstellt. **xxx** bezeichnet den Berichtnamen, der im Performance Manager festgelegt ist:

- **xxx.dat**
- **xxx.ind**
- **xxx.names**

Wenn Sie die Berichteinstellungen im Performance Manager löschen, werden diese Dateien auch gelöscht.

Wenn Sie **Maximum number of recorded report entries** nicht einstellen für die Berichtdefinition im Performance Manager, oder wenn Sie Berichte über einen längeren Zeitraum durch Server-Abfragen in kurzen Zeitabständen ausgeben, kann es zu Speicherplatzeinschränkungen kommen, weil eine Datei zu groß wird. Um dies zu vermeiden, sollten Sie dafür sorgen, dass die Einstellungen für die Anzahl der Eingaben und der Zeitabstand für die Berichtausgabe korrekt gesetzt sind.

3.5.12 Temporäre Datei im Verzeichnis /tmp

Wenn der ServerView Linux-Agent startet, wird eine temporäre Datei mit einer Größe von 0 Bytes und mit dem Namen **S.xxxxxx** (**xxxxxx** ist eine beliebige alphanumerische Zeichenkette) im Verzeichnis **/tmp** erstellt.

Diese Datei ermöglicht die Kommunikation zwischen dem Sub-Agenten des ServerView-Agenten und snmpd.

Der Ort für diese Datei kann nicht geändert werden.

Außerdem kann es sein, dass der ServerView Linux-Agent nicht korrekt funktioniert, wenn Sie diese Datei manuell löschen.

3.5.13 Quellname von "syslog"

Wenn der ServerView-Agent einen Hardware-Fehler erkennt, wird dieser in "syslog" berichtet. Der Quellname für die von ServerView-Agenten berichteten Ereignisse ist **ServerView**.

3.6 APC-USV konfigurieren

Die folgende Beschreibung ist nur gültig für PRIMERGY.

Voraussetzung für die Überwachung der USV ist die Installation des entsprechenden Agenten (APC) auf dem Server. Bei einer APC-USV mit Web-Karte ist der entsprechende SNMP-Agent auf der Web-Karte vorinstalliert.

Um die existierende USV-Konfiguration im Operations Manager anzuzeigen, muss sie über das Installationsprogramm eingetragen werden. Eine

automatische Erkennung ist zurzeit noch nicht implementiert. Jeder USV-Eintrag enthält dann u.a. die von ihm überwachte Hardware.

Für die USV-Konfiguration steht das Utility **oemups** zur Verfügung. Um USV-Einträge hinzuzufügen, geben Sie folgendes Kommando ein:

```
oemups -a
```

Daraufhin werden die Parameter **Vendor Name**, **UPS Type**, **IP Address** und **Cabinet ID** abgefragt. In diesen Feldern werden zunächst die Standardwerte (**American Power Conversion**, **APC UPS, 0.0.0.0, 0**) angezeigt. Geben Sie bei **IP Address** die IP-Adresse des Servers oder die IP-Adresse der USV mit Web-Karte ein.

Alle vorhandenen USV-Einträge listen Sie über folgendes Kommando auf:

```
oemups -l
```

Einen USV-Eintrag löschen Sie über das Kommando:

```
oemups -d <Nummer des USV-Eintrags>
```

Beachten Sie, dass alle Änderungen erst nach einem Neustart des Servers aktiv werden.